Impact of Security on QoS in Communication Network

Jianyong Chen, Cunying Hu, Huawang Zeng
Department of Computer Science and Technology,
Shenzhen University,
Shenzhen, P.R. China, 518060.
jychen@szu.edu.cn

Jun Zhang
Department of Computer Science,
SUN Yat-sen University,
Guangzhou, P.R. China, 510275.
junzhang@ieee.org

***Abstract*—With the development of both economy and society, service always requires higher and higher security and quality. However, since security services always induce extra resource consumption, QoS may descend evidently. It is important and essential to find optimal solutions that can not only achieve enough level of security, but also meet as high QoS as system can. In this paper, we propose an entity, named QoS amending function, which is used to evaluate the end-to-end delay induced by security in communication network. Moreover, an adaptive immune algorithm is used to obtained optimal parameters on both security and QoS. Simulations show that the proposed model is effective to achieve optimal balance between security and QoS.**

Keywords-QoS amending function; security assurance level (SAL); QoS; immune algorithm

I. INTRODUCTION

Traditionally, Quality of Service (QoS) and security had been regarded as separate capabilities in communication network. However, with the development of research, it is discovered that both of them strongly correlate each other [1]. On one hand, stable QoS needs enough protection to resist diversified attack [2] and avoid congestion of the network due to successful attacking. On the other hand, security service always has an obvious impact to QoS, such as additional delay caused by proceeding of encryption or authentication. It is very important and essential to ensure security in wireless network, especially in Ad Hoc network [3], since the wireless channel opens on the air and attackers are more easily to intrude the transmitting information. Moreover, the limited bandwidth of wireless channel augments the impact of security on QoS greatly. Therefore, the impact of security on QoS should be considered to better satisfy customer's requirements [4].

Several studies have been reported on the interaction between QoS and security in networks. References [5], [6], [7] study the impact of challenge/response authentication on QoS in wireless LANs. Reference [5] investigates the impact of security levels, mobility and traffic patterns on overall system performance in terms of authentication cost, latency and the call dropping probability. Reference [6] introduces a mechanism for a distributed dynamic management system. It aims to maximize QoS and/or security while maintaining a minimum level of security and/or QoS consumption, even as network resource availability changes. Reference [7] specifies a tradeoff between security and QoS through the choice of available security configurations.

Although the above research provided an analysis of the resource consumption caused by authentication and encryption, none of them further studies the quantitative impact of security on QoS.

On the other hand, Immune algorithm (IA) has been developed by the enlightenment of human immune system. In recent years, IA has been widely applied in pattern recognition, function optimization, and network intrusion detection. In our research, the goal is to get minimal delay and high security level under given condition. It can be described using a mathematical model with multi-objective optimization problems. In order to find optimal solutions, immune algorithm [10] is used with parameters of authentication rate and key length.

The rest of this paper is organized as follows. A QoS amending module is introduced in Section 2. In section 3, the impact of both encryption and authentication are studied separately. In section 4, immune algorithm is used to get the optimal solutions at different delay requirements from users. Finally, a conclusion is presented in Section 5.

II. QOS AMENDING MODULE

In the paper, the QoS amending model can be described as Fig. 1.

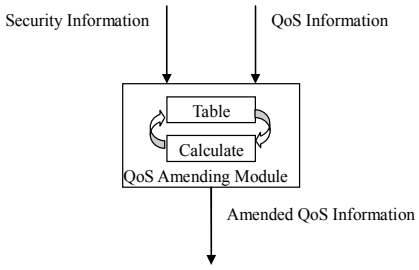

Figure 1. Interface of QoS Amending Module.

The interfaces of the QoS amending module are described as follows: there are at least two kinds of input interfaces, i.e., input interface of QoS information and input interface of security information. In addition, there is one type of output interface, that is, output interface of QoS information. The input interface can include one or more physical or logistic interfaces in practical applications. QoS information includes QoS parameters and other related

978-0-7695-3610-1/09 $25.00 © 2009 IEEE
DOI 10.1109/NSWCTC.2009.279

information. Security information similarly contains security parameters and other related information with security.

The process of QoS amending method includes parameters collecting, parameters amending and parameters outputting. They are described as follows:

Parameters collecting: both of security and the QoS information are transmitted to the QoS amending module.

Parameters amending: the QoS amending module amends the input QoS information according to the input security information with particular algorithms, policies or manual configuration. The module consists of two segments: Table unit and Evaluation unit. Table unit is used to store parameters of the impact of security on QoS. Evaluation unit can amend the QoS parameters according to the security parameters. When the QoS amending module receives the information about QoS and security, it, firstly, looks up the table to get the amending values directly. If there are results corresponding to input information in the table, the Table unit sends the results to the output interface. Otherwise, it sends input information to the Evaluation unit to execute calculation. Then, the results are sent to both the Table unit for storage and output interface. With the assistance of Table unit storage, the amended QoS parameters can be directly obtained from the Table unit if the same situation occurs again later.

Parameters outputting: the amended QoS information is sent out from the output interface.

III. System Performance Analysis

In this section, we introduce two security methods: encryption and authentication. Their effects on security and QoS are studied separately.

It is well known that user authentication and data encryption are two main security mechanisms, and they mainly determine SAL. Data encryption is a key factor of SAL. The SAL is different by using different encryption algorithms with the same key length, or using the same encryption algorithm with different key length. However, it also brings additional time delay which is main element of QoS [8]. Authentication is another factor of SAL. It can not only result in evident overhead, but also increase call dropping probability.

If the end to end communication consists of data encryption and decryption, data transmission and authentication, the time delay T is equal to the sum of encryption and decryption time, transmission time and authentication time. Since both of authentication and encryption have an impact on the security [5], it is supposed that the SAL can be determined by minimum between SAL of encryption and SAL of authentication. The final time delay T and SAL L can be expressed as (1) and (2):

$$T = t_{net} + t_k + t_a \tag{1}$$

$$L = min(l_k, l_a) \tag{2}$$

Here, t_{net} is delay requirement from user without security services. t_k is encryption and decryption time. t_a is authentication time in every packet transmission. l_k and l_a are the SALs of encryption and authentication respectively.

A. Encryption

Data encryption can not only protect user's communication content, but also resist various attacks. Moreover, encryption can also prevent the most important information from leakage, especially in wireless networks. However, it also induces extra consumption and causes additional time delay [8].

In the paper, we adopt AES (Advanced Encryption Standard) as encryption algorithm. AES is proclaimed by National Institute of Standards and Technology (NIST) in 2001, and has been widely adopted by network hardware and software' suppliers. AES is capable to handle key sizes of 128, 196 and 256 bits.

1) Effect of Encryption on Security: The SAL of a given cipher system is related to the security of its algorithm and key length [9]. It is assumed that encryption algorithm has enough safety, which means there is no better way to decipher the cipher system than exhaustive attack. Therefore, it is not difficult to calculate attack complex degree. If the key length is 8 bits, there are 2^8=256 possible keys, so it needs to try 256 times in worst situation to get correct key. When the key length is k_{len}, it needs to try 2^{klen} times. Therefore, we can conclude that the longer the key length is, the more trial times are needed, which indicates that the SAL is higher.

According to the practical instance, we can assume that SAL is 1 when the key length is shortest. The encryption security level l_k can be denoted:

$$l_k = 2^{k_{len}/k_{min}} - 1 \tag{3}$$

Where, k_{min} is the shortest key length. Note that the range of SAL is from 0 to 3.

2) Effect of Encryption on Delay: When using AES to encrypt and decrypt the same message, the encryption and decryption time of AES exhibits linear change along with the key length according to [8]. By this means, the encryption delay and decryption delay t_k can be determined by:

$$t_k = a * k_{len} + b \tag{4}$$

Where，a is proportional coefficient which stands the rate of the delay, b is a constant and may be different at different hosts.

B. Authentication

In order to validate users' identities and provide security for users，authentication is always used as an initial process to authorize users for establishing and maintaining trusted communications. By rejecting unlawful authenticated users, authentication can protect network data and users.

In the paper, we adopt challenge/response authentication at security level 4 is used to certify legal users [5]. The process is as follow: when an AP (access point) receives one authentication request from users, it implements with shared SA (security association). It is noteworthy that encryption is independent to the authentication in point of both delay and security.

1) Effect of Authentication on Delay: Up to now, there is only some qualitative studies on relation between authentication and SAL, but very little work has been done in the quantitative analysis of their relationship. It is very difficult to quantify authentication accurately according to the process of authentication, or metrics of security, such as data integrity and data confidentiality. Therefore, we use the arrival rate of authentication, which is defined as authentication times in one minute to evaluate SAL quantitatively.

It is a general agreement that the more the times of authentication is, the higher the security level is. As the authentication rate changes, the SAL changes accordingly. For simplicity, it is assumed that authentication rate is proportional to the SAL, and a linear function is adapted to describe the relationship between authentication and SAL. It is carried out as follow:

$$l_a = r_a * e \tag{5}$$

Where l_a is SAL of authentication, and the authentication rate is r_a, e is proportional coefficient of authentication rate.

2) Effect of Authentication Rate on Delay: The authentication service is always provided at the beginning of a communication. Once the authentication is finished, the following communicating processes are basically unaffected by authentication. Authentication delay is the time between sending an authentication request and receiving the reply [5], and proportional to the authentication rate. By this means, the authentication delay T_a and t_a can be denoted as follows:

$$T_a = c * r_a + d \tag{6}$$

$$t_a = r_a * T_a / (1/T) = r_a * T_a * T \tag{7}$$

Here, c is proportional coefficient, and d is a constant and is changed with different network. $r_a * T_a$ represents the sum of authentication time in a time unit.

At last, the amending delay can be obtained by substituting (7) into (1), which is expressed by:

$$T = (t_{net} + t_k) / (1 - r_a * T_a) \tag{8}$$

IV. SIMULATIONS

In this section, simulations mainly focus on Evaluation unit which evaluate the impact of security on QoS.

A. Assumptions and Parameters

Simulations are performed with PIV 2.0GHZ PC, and encrypt on a 1500B message, Ethernet packet. The challenge/response authentication at SAL 4 is implemented in communication [5], and we suppose that the arrival rate of call is equal to authentication rate. By this means, c and d can be determined. In summary, the parameters to evaluate the security and delay are shown in Table I and Table II.

TABLE I. PARAMETERS FOR EVALUATION ON DELAY

Parameters for Delay				
a	***b***	***c***	***d***	t_{net}
0.0195	7.5	4e+007	296.7	[20,40,60,80,100]

TABLE II. PARAMETERS FOR EVALUATION ON DELAY AND SAL

Parameters for Delay and SAL			
k_{min}	***e***	r_a	K_{len}
128	9e+005	[0,0.2]	[0,256]

If there is no item matched in Table unit with given t_{net} and SAL, Evaluation unit calculates the amending delay with different SALs, and updates the items in Table unit. In practice, people expect higher SAL and shorter delay under certain network resource. In the paper, we use immune optimization agorithm to optimize (2) and (8), and get the corresponding values of key length and authentication rate (k_{len}, r_a), which can be used to configure the security service in practical applications.

B. Impact of SAL to Amending Delay

The impact of SAL on delay is shown in Fig. 2. The key length and authentication rate at optimal values are shown in Fig. 3.

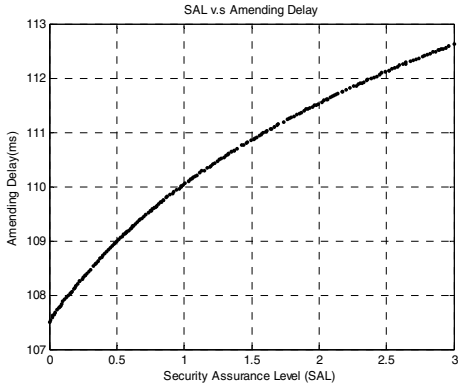

Figure 2. SAL and Amending Delay (t_{net} = 100).

Fig.2 shows that the amending delay increases with the increase of the SAL. This trend is due to the increase of key length and authentication rate, causing more encryption time and authentication time. When the SAL moves from 1 to 2,

additional delay increases around 1.4898ms. Similarly, if the SAL moves from 2 to3, the additional delay is 1.0871ms which is only 72.97% of the former one.

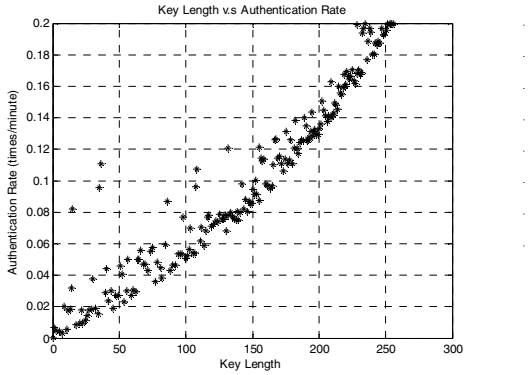

Figure 3. Key length and authentication rate.

Evidently, the increase rate of SAL is lager than that of delay. As shown in (3) and (5), the SAL of encryption is exponential growth with key length, and the SAL of authentication is proportional to the arrival rate of authentication request. Moreover, the impact of security on delay is mainly caused by encryption, and (4) shows linear variation of the encryption delay with key length. Thus, it resulted in the above observation.

Fig. 3 reveals that authentication rate increases basically similar with key length. This is because that the SAL is determined by minimum of l_k and l_a, as shown in (2). In order to get the SAL as large as possible, their increments become similar. Moreover, since encryption is independent of authentication, there are multiple optimal combinations between k_{len} and r_a for a given SAL. Therefore, the points of (k_{len}, r_a) have relative large distribution, as shown in Fig. 3.

C. Impact of Delay Requirement from users

Fig. 4 shows impact of delay requirement from users under different SALs.

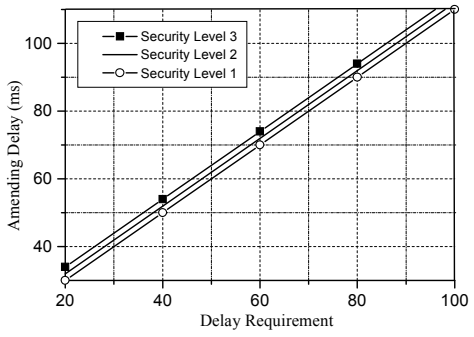

Figure 4. Amending delay and delayrequirement from users.

The simulations show that the amending delay increases with the delay requirement linearly. This is because that the authentication rate and key length is basically constant at a given SAL, and the amending delay is proportional to the delay requirement, as is described in (8). Moreover, a higher SAL corresponds to longer delay. For example, if the SAL moves from 1 to 2, the additional delay is 1.4898ms under the same delay requirement.

V. CONCLUSION

In this paper, we proposed an entity, named QoS amending function, to calculate the impact of security on QoS. The outputs are used to amend the original QoS parameters before they are executed by the related QoS enforcement functions. The system performance is analyzed with respect to end-to-end delay and SAL. Furthermore, the paper studied the impacts of encryption and authentication on SAL and delay. At last, to get the minimum delay and the highest SAL, we used immune algorithm to optimize key length and authentication rate. Simulations show that the proposed model is effective to get the optimal solutions under different configurations.

ACKNOWLEDGMENT

The work was jointly supported by the National Natural Science Foundation of China (Grant No: 60703112) and the Science and Technology Plan of Shenzhen City under the project number QK200610.

REFERENCES

[1] Fathi, H. Kobara, K, Chakraborty, SS, et al., “On the impact of security on latency in WLAN 802.11b” SCI, pp. 1752-1756, 2005.

[2] Marek Hejmo, Brian L. Mark, Charikleia Zouridaki, and Roshan K. Thomas, “Design and analysis of a Denial-of-Service-Resistant Quality-of-Service signaling protocol for MANETs”, IEEE Trans. on Vehicular Technology, 2006, V55, pp.743-751..

[3] Bin Lu, Udo W. Pooch, “Security in QoS signaling systems for Mobile Ad Hoc Networks”, IEEE WiMob’2005, August 2005, V3, pp.213-220.

[4] Sandrine Duflos*, Brigitte Kervella, Valérie C. Gay, “Considering Security and Quality of Service in SLS to improve Policy-based Management of Multimedia Services”, Six International Conference on Networking (ICN’07), April 2007, pp. 39-39.

[5] Wei Liang, Wenye Wan, “A Quantitative study of authentication and QoS in wireless IP networks” Proceedings IEEE (INFOCOM 2005), March 2005, V2, pp1478-1489.

[6] ZhengMing Shen and Johnson P Thomas, “Security and QoS self-optimization in Mobile Ad Hoc Networks” IEEE Trans. on Mobile Computing, 2008, V.7, pp.1138-1151.

[7] Lindskog, S; Brunstrom, A; Faigl, Z, et al, “Providing tunable security services:an IEEE 802.11i example” Securecomm and Workshops 2006, 2006, pp. 1-10.

[8] Wenbo He, Klara Nahrstedt, “An integrated solution to delay and security support in wireless networks”, IEEE Wireless Communications and Networking Conference (WCNC 2006), 2006, V4, pp. 2211-2215.

[9] Bruce Schneier , “Applied Cryptography Protocols, algorithms, and source code in C (Second Edition) ”, 2006, John Wiley & Sons.

[10] Maoguo Gong, Licheng Jiao, Haifeng Du and Liefen Bo. “Multi-objective immune algorithm with nondominated neighbor-based selection”. Evolutionary Computation (MIT Press), 2008,Vol. 16, No. 2, pp.225-25.